IN THE CLAIMS

Please cancel claims 7-14.

Please amend claims 1, 3, 5, and 15 as follows:

1.(Currently Amended) A method for adjusting an m-bit CRC of a sub-message, wherein ~~a~~the CRC generating polynomial for generating the m-bit CRC is primitive or irreducible and the sub-message corresponds to a composite sub-message having n trailing zeroes, where m and n are integers, comprising:

storing the m-bit CRC in an m-bit memory location;

examining each bit of N, where N is a binary representation of a result of~~equals~~ n mod $(2^m - 1)$, in order from ~~a~~the most significant bit to ~~a~~the least significant bit; the examining act for each examined bit comprising:

finite field squaring the contents of the m-bit memory location, and;

if the examined bit equals one, advancing the contents of the m-bit memory location to ~~a~~the next state as determined by the Galois field defined by the CRC generating polynomial.

2.(Original) The method of claim 1, wherein the CRC generating polynomial is a primitive polynomial.

3.(Currently Amended) The method of claim 1, wherein the CRC generating polynomial is an irreducible polynomial.

4.(Original) The method of claim 1, wherein for each examined bit equaling one, the finite field squaring act and the advancing the contents act are performed simultaneously.

5.(Currently Amended) A method for adjusting an m-bit CRC of a sub-message, wherein the sub-message corresponds to a composite sub-message having n trailing zeroes ~~and the m-bit CRC is equal or congruent to one~~, where m and n are integers, comprising:

storing the m-bit CRC in an m-bit memory location;

examining each bit of N, where N is a binary representation of a result of~~equals~~ n mod (2^m-1), in order from a~~the~~ most significant bit to a~~the~~ least significant bit; the examining act for each examined bit comprising:

finite field squaring the contents of the m-bit memory location, and;

if the examined bit equals one, advancing the contents of the m-bit memory location to a~~the~~ next state as determined by a~~the~~ Galois field defined by a~~the~~ CRC generating polynomial for generating the m-bit CRC.

6.(Original) The method of claim 5, wherein the CRC generating polynomial is neither primitive nor irreducible.

7. – 14.(Cancelled)

15.(Currently Amended) A method of advancing an m-bit sequence through n states of a Galois field generated by a primitive or irreducible polynomial of degree m, where m and n are integers, comprising:

storing the m-bit sequence in an m-bit memory location;

examining each bit of N, where N is a binary representation of a result of~~equals~~ n mod (2^m-1), in order from a~~the~~ most significant bit to a~~the~~ least significant bit; the examining act for each examined bit comprising:

finite field squaring the contents of the m-bit memory location, and;

if the examined bit equals one, advancing the contents of the m-bit memory location to a~~the~~ next state as determined by the Galois field.

16.(Original) The method of claim 15, wherein the polynomial is a primitive polynomial.

17.(Original) The method of claim 15, wherein the polynomial is an irreducible polynomial.